

Cedefop record of processing activity

Record of Cedefop activities processing personal data, based on Article 31 of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and Decision 1247/2002/EC.

Nr.	Item	Description
<i>Establishment and management of staff personal files</i>		
1.	Last update of this record	22/10/2025
2.	Reference number	RB2026-1948425193-2549
3.	Name and contact details of controller	Cedefop – European Centre for the Development of Vocational Training Postal address: Cedefop Service Post, Europe 123, 570 01 Thessaloniki, GREECE Telephone: (+30) 2310-490111 Email: info@cedefop.europa.eu Responsible department or role: DRS/HR Email: hr-data-protection@cedefop.europa.eu
4.	Contact details of DPO	data-protection-officer@cedefop.europa.eu
5.	Name and contact details of joint controller (where applicable)	N/A
6.	Name and contact details of processor (where applicable)	- The Paymaster's Office of the Commission (PMO), including PMO Transfer-In Sector and PMO Pension Sector Contact details may be found on the respective webpage: https://paymaster-office.ec.europa.eu/services-topic/salaries-and-allowances_en - The Joint Sickness Insurance Scheme (JSIS) Contact details may be found on the respective webpage: https://paymaster-office.ec.europa.eu/services-topic/health-and-accident-insurance-jsis_en - The European Personnel Selection Office (EPSO) Contact details may be found on the respective webpage: https://eu-careers.europa.eu/en/contact-us

7.	Very short description and purpose of the processing	Establishment and management of staff personal files: data collection starts when the future staff member has accepted Cedefop's job offer from AIPN. The data are provided by the data subject at the request of the HR Service. The new staff member is assigned a unique personal number. The personal file is managed by the HR Service and updated as necessary. It contains all records (in paper or electronic form) relating to the employment at Cedefop, including selection and recruitment, rights and obligations, career development, administrative status, social security, end of service, legal proceedings, etc. Staff must inform the HR Service of any change in their administrative status or family situation. In addition, HR periodically requests staff to confirm or review this information. The collection of documents to be included in the personal files finishes when the work relationship of the data subject with Cedefop ends. In the event of an inter-institutional transfer and at the request of the recruiting institution, Cedefop transmits the personal file of the staff member concerned to the recruiting institution. The legal basis of the procedure is: • The lawfulness of the processing is defined by Articles 5(1)(a) and Articles 10(2)(b) and (h) of Regulation (EU) 2018/1725. • Article 26 of the Staff Regulations and Article 11 of the Conditions of Employment of Other Servants regarding personal file. • Articles 28 and 33 of the Staff Regulations and Articles 12, 13, 82, 83, 128 and 129 of the Conditions of Employment of other servants regarding medical examination before appointment.
8.	Description of categories of persons whose data Cedefop processes and list of data categories	Data subjects: • Officials (OFFs), temporary agents (TAs), and contract agents (CAs), who are all currently, or have been, in employment with Cedefop. Data categories: • Personal information such as but not limited to: surname, first name, nationality, date of birth, address, e-mail address, phone numbers,

		criminal record, marital status, family situation (e.g. data of spouse, partner, dependent children, and other dependents), financial data (e.g. tax declarations), unique personal number. • Data related to the selection procedure such as: application and supporting documents (e.g. previous employment contracts and payslips, CV, offer of the post). • Documents concerning administrative status, reports on performance (e.g. appraisal reports, promotion/reclassification decisions), and pension rights. Special categories of sensitive data within the meaning of Article 10 of the EUDPR¹: • Data used to determine the rights and grant the allowances of the data subject: e.g. marriage certificate, birth certificate of children. • Data concerning health: e.g. medical fit to work certificates. • Data relating to suspected offences, offences, criminal convictions or security measures: e.g. criminal record. • If applicable, data on disciplinary measures and complaints.
9.	Time limit for keeping the data	The administrative retention period is 8 years after the extinction of all rights of the person concerned and of any dependants, and for at least 100 years after the recruitment of the person.
10.	Recipients of the data	Internal recipients: • HR staff. • Staff members can access their personal files, both paper (upon request) and electronic versions (from Cedefop records and document management system). • Cedefop's Executive Director may access data through the HR Service for a specified purpose and on an as-needed basis. A log is maintained to record all consultations.

¹ Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation.

		• Finance Service and Accountancy, responsible for processing the payments, can access relevant data only such as: staff name, personal number and NUP, contract type and grade, ID cards or passport, and bank account details. • Procurement Service, for the nomination of the opening and evaluation committees, can access staff name, contract type and grade. • Cedefop's staff internally responsible for audit and review activities, as well as staff of contractors providing audit and review services to Cedefop, may access the personal data collected through this processing operation to the extent necessary for carrying out their duties. External recipients: • The Paymaster's Office of the Commission (PMO), which establishes the salaries, can access relevant data only such as: staff name, date of birth, gender, nationality, place of origin, civil status, contract type and grade, contract duration, career (step changes, promotions/reclassifications), ID cards or passports, bank account details, restaurant costs, date of marriage/partnership/divorce, name and dates of birth of family members and dependents, relevant certificates (birth, marriage, etc), income of spouse/recognised partner, and other allowances received from other sources. PMO Transfer-In Sector: staff name, date of birth, personal number and NUP, contract type and grade, career, info on CCP, and ID cards or passports PMO Pension Sector: staff name, date of birth, nationality, personal number and NUP, place of origin, contract type and grade, career, info on CCP, ID cards or passports, private contact details, bank account details, info about family situation and dependents, info on transfer in, salary slips, and income of spouse/recognised partner. • The Joint Sickness Insurance Scheme (JSIS) can access relevant data only such as at recruitment: staff name, date of birth, gender, nationality, mother tongue, civil status, contract type and grade, contract duration, ID cards or passport, private contact details, bank account details, date of
--	--	---

		marriage/partnership/divorce, name and dates of birth of family members and dependents, and income of spouse/recognised partner; and during career: any change in family status or dependents during the contract period and until departure/retirement. • The European Personnel Selection Office (EPSO) can access staff name, date of birth, and language/degree certificates. • Other EU agencies/institutions: personal files may be transferred following inter-agency mobility of a Cedefop staff member, at the request of the agency and with the consent of the staff member concerned.
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	N/A
12.	General description of security measures where possible.	Cedefop implements a number of technical and organisational security measures to address, among others, online security (firewall, URL filtering, antivirus programs), risk of data loss and alteration (back-up and restore policy), as well as to grant access to its information and documents only to authorised users based on a 'need to know' principle (through authentication and authorisation procedures, encryption). Cedefop has also put in place appropriate incident handling and personal data breaches procedures. Compliance with these measures is ensured through Cedefop's ICT Use and Security Policy, which is regularly reviewed for improvements. Active paper personal files are kept in locked cabinets under the control of the HR Service. Paper personal files of non-active staff are also stored in locked cabinets up to 3 years after departure, after which they are moved in the Archives room (which is also under strict access control). Any personal data of special categories within the meaning of Article 10 of the EUDPR is protected by the application of the corresponding sensitivity labels and the special technical measure of "Double-key encryption" (DKE). All data processing is confidential. Communication of data is restricted to those persons who "need to know" for the performance of their duties.

13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement published on the Cedefop webportal.
-----	--	---